IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE: EQUIFAX, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2800 1:17-MD-2800-TWT ALL ACTIONS

NOTICE OF SERVICE OF SUBPOENA TO MASTERCARD INTERNATIONAL INCORPORATED

The undersigned counsel for The Financial Institution Plaintiffs, pursuant to Federal Rule of Civil Procedure 45(a)(4), hereby certifies that a Subpoena for the Production of Documents will be served upon Mastercard International Incorporated. A copy of the Subpoena is attached hereto.

Respectfully submitted this 7th day of March, 2019.

CONLEY GRIGGS PARTIN LLP

/s/ *Ranse M. Partin*
RANSE M. PARTIN
Georgia Bar No. 556260

4200 Northside Parkway, NW
Building One, Suite 300
Atlanta, Georgia 30327
(404) 467-1155
ranse@conleygriggs.com

ATTORNEYS FOR THE FINANCIAL INSTITUTION PLAINTIFFS

CERTIFICATE OF SERVICE

I hereby certify that I have this date electronically filed the foregoing **NOTICE OF SERVICE OF SUBPOENA TO MASTERCARD INTERNATIONAL INCORPORATED** with the Clerk of Court using the CM/ECF system which will automatically send email notification of such filing to the following attorneys of record:

Stewart Haskins, III, Esq.
Phyllis B. Sumner, Esq.
David Balser, Esq.
King & Spalding, LLP
1180 Peachtree Street, NW
Atlanta, GA 30309
shaskins@kslaw.com
psumner@kslaw.com
dbalser@kslaw.com
(Counsel for Defendant Equifax)

This 6th day of March, 2019.

CONLEY GRIGGS PARTIN LLP

/s/ *Ranse M. Partin*
RANSE M. PARTIN
Georgia Bar No. 556260
4200 Northside Parkway, NW
Building One, Suite 300
Atlanta, Georgia 30327
(404) 467-1155
ranse@conleygriggs.com

ATTORNEYS FOR THE FINANCIAL INSTITUTION PLAINTIFFS

AO 88B (Rev. 02/14) Subpoena to Produce Documents, Information, or Objects or to Permit Inspection of Premises in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of Georgia

In Re Equifax, Inc. *Plaintiff* v. Customer Data Security Breach Litigation *Defendant*	)	MDL DOCKET NO. 2800 Civil Action No. 1:17-md-2800-TWT ALL ACTIONS

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Mastercard International Incorporated, c/o CT Corporation System, 289 S. Culver St., Lawrenceville, GA 30046

(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: SEE ATTACHED SCHEDULE A AND STIPULATION AND ORDER FOR THE PRODUCTION OF DOCUMENTS AND ESI.

Place:	Date and Time:
Martin S. Hyman, Esq.; Golenbock Eiseman Assor Bell & Peskoe, 711 Third Avenue, New York, NY 10017	04/06/2019 10:00 am

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 03/07/2019

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

/s/ Ranse M. Partin

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* The Financial Institution Plaintiffs, who issues or requests this subpoena, are:

Ranse M. Partin, Conley Griggs Partin LLP, 4200 Northside Pkwy, NW, Bldg. One, Suite 300, Atlanta, GA 303327

(404) 467-1155 ranse@conleygriggs.com

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 1:17-md-2800-TWT

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Print Save As... Add Attachment Reset

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

SCHEDULE A

I. DEFINITIONS

1. "Financial Institution Plaintiffs" means the plaintiffs identified in Case Management Order No. 2 filed on January 10, 2018 in *In re: Equifax, Inc., Customer Data Security Breach Litigation*, No. 1:17-md-2800-TWT (N.D. Ga.) (Dkt. 87).

2. "Consumer Plaintiffs" means the plaintiffs identified in Case Management Order No. 2 filed on January 10, 2018 in *In re: Equifax, Inc., Customer Data Security Breach Litigation*, No. 1:17-md-2800-TWT (N.D. Ga.) (Dkt. 87).

3. "Plaintiffs" means the Financial Institution Plaintiffs and/or the Consumer Plaintiffs.

4. "Equifax" and "Defendant" mean Equifax, Inc., and any of its directors, officers, employees, partners, members, representatives, agents (including attorneys, accountants, consultants, investment advisors or bankers), and any other person purporting to act on their behalf. In the case of business entities, these defined terms include parents, subsidiaries, affiliates, predecessor entities, successor entities, divisions, departments, groups, acquired entities and/or related entities or any other entity acting or purporting to act on their behalf.

5. "Acquiring Bank" means any bank, credit union, financial entity, or organization that acquires or processes any Payment Card transactions.

6. "Action" or "Litigation" means the case captioned *In re: Equifax, Inc., Customer Data Security Breach Litigation*, 1:17-md-2800-TWT (N.D. Ga.), and each of the constituent actions transferred to and/or consolidated therein.

7. "Communication" means the transmittal (in the form of facts, ideas, thoughts, opinions, data, inquiries or otherwise) expressed by any means, and includes, without limitation,

correspondence, memoranda, reports, presentations, face-to-face conversations, telephone conversations, text messages, instant messages, voice messages, negotiations, agreements, inquiries, understandings, meetings, letters, notes, telegrams, mail, email, and postings of any type.

8. "Complaint" means the operative Consolidated Class Action Complaints to be filed in the Action, as well as any previously-filed complaints consolidated before the Northern District of Georgia in the Litigation.

9. "Computer Network" means the data network that connects the components of Your Computer System(s) with Equifax's Computer Systems;

10. "Dispute Portal" means Equifax's customer dispute portal;

11. "Computer System" Includes any server (whether physical or virtual), desktop computer, laptop computer, tablet computer, point-of-sale system, debit or credit card reader, payment processing system, smart phone, cellular telephone, device containing a central processing unit, networking equipment, internet site, intranet site, and the software, programs, applications, scripts, operating systems, or databases used to control, access, store, add, delete, or modify any information stored on any of the foregoing non-exclusive list.

12. "Concerning" means any Document which explicitly or implicitly, in whole or in part, compare, were received in conjunction with, or were generated as a result of the subject matter of the request, including all Documents which reflect, refer, record, are in regard to, in connection with, specify, memorialize, relate, describe, discuss, consider, constitute, embody, evaluate, analyze, refer to, review, report on, comment on, impinge upon, or impact the subject matter of the request.

13. "Customer Identifying Information" means information about Equifax's customers or potential customers including, without limitation, name, address, phone number, email address,

date of birth, Social Security Number, account number (*e.g.*, bank, debit or credit card), Driver's License, Passport or other government identification number.

14. "Data Breach" means the unauthorized access to Customer Identifying Information that Equifax publicly announced on or about September 7, 2017.

15. "Document" is defined to include any document and ESI stored in any medium, and is synonymous in meaning and equal in scope to the usage of this term in Federal Rule of Civil Procedure 34(a)(l)(A), including, without limitation, electronic or computerized data compilations, electronic chats, instant messaging, email, other electronic stored information from personal computers, sound recordings, photographs, and hard copy documents maintained in your personal files.

16. "Electronic Media" means any magnetic, optical, or other storage media device used to record ESI including, without limitation, computer memory, hard disks, floppy disks, flash memory devices, CDs, DVDs, Blu-ray disks, cloud storage (*e.g.*, DropBox, Box, OneDrive, and SharePoint), tablet computers (*e.g.*, iPad, Kindle, Nook, and Samsung Galaxy), cellular or smart phones (*e.g.*, BlackBerry, iPhone, Samsung Galaxy), personal digital assistants, magnetic tapes of all types or any other means for digital storage and/or transmittal.

17. "Employee" means any current or former officer, director, or other person who is or was employed by you.

18. "ESI" or "Electronically Stored Information" means information that is stored in Electronic Media, regardless of the media or whether it is in the original format in which it was created, and that is retrievable in perceivable form and includes, without limitation, metadata, system data, deleted data, and fragmented data.

19. "Financial Institution" means banks, credit unions, and other institutions that issue credit cards, debit cards, bank cards or any other payment cards that were subject to the Data Breach.

20. "Identify," with respect to Persons, means to give, to the extent known, the Person's full name, present or last known address, telephone numbers, and when referring to a natural person, additionally, the present or last known place of employment. Once a Person has been identified in accordance with this subparagraph, only the name of that Person need be listed in response to subsequent discovery requesting the identification of that Person.

21. "Identify," with respect to Documents, means to give, to the extent known, the (a) type of document; (b) general subject matter; (c) date of the document; (d) author(s); (e) addressee(s); and (f) recipient(s).

22. "Including" means "including but not limited to" and "including without limitation."

23. "Issuing Bank" means any bank, credit union, financial entity, or organization that issues, or causes to be issued, Payment Cards.

24. "Meeting" means the contemporaneous presence, whether in person or through any means of communication, of any natural persons, whether or not such presence was by chance or prearranged, and whether or not the meeting was formal or informal, or occurred in connection with some other activity.

25. "Payment Card Data" means all information associated with a credit or debit card including, without limitation, customer name, credit or debit card number, card expiration date, CVV, debit card personal identification numbers ("PIN"), magnetic strip information, and any Customer Identifying Information.

26. "Payment Processing Company" includes, without limitation, Visa, Inc. ("Visa"), MasterCard Corporation ("MasterCard"), American Express Company ("AmEx"), Discover Financial Services ("Discover"), any other company that processes credit or debit card payments, and each of their respective directors, officers, employees, partners, members, representatives, agents (including attorneys, accountants, consultants, investment advisors or bankers), and any other person purporting to act on their behalf. In the case of business entities, these defined terms include parents, subsidiaries, affiliates, predecessor entities, successor entities, divisions, departments, groups, acquired entities and/or related entities or any other entity acting or purporting to act on their behalf.

27. "PCI Standards" means the Payment Card Industry ("PCI") Data Security Standards ("DSS").

28. "Person" means any natural person or any business, legal or governmental entity or association.

29. "Referring" or the phrase "relating to" means all documents which comprise, explicitly or implicitly refer to, were reviewed in conjunction with, or were created, generated, or maintained as a result of the subject matter of the request, including, without limitation, all documents which reflect, record, memorialize, embody, discuss, evaluate, consider, review, or report on the subject matter of the request.

30. "Security" means the protection of Computer Systems, POS Technology, and/or Payment Card Data from unauthorized access, manipulation, modification, misuse, transfer, exfiltration, and/or destruction.

31. "Comcast Corporation" "you," or "your" means Comcast Corporation and any of its directors, officers, employees, partners, members, representatives, agents (including attorneys,

accountants, consultants, investment advisors or bankers), and any other person purporting to act on their behalf. In the case of business entities, these defined terms include parents, subsidiaries, affiliates, predecessor entities, successor entities, divisions, departments, groups, acquired entities and/or related entities or any other entity acting or purporting to act on their behalf.

II. RULES OF CONSTRUCTION

1. "Any," "all," and "each" shall be construed as any, all and each.

2. The connectives "and" and "or" shall be construed either disjunctively or conjunctively as necessary to bring within the scope of the discovery request all responses that might otherwise be construed to be outside of its scope.

3. The singular form of a noun or pronoun includes the plural form and vice versa.

4. The use of any tense of any verb shall also include within its meaning all other tenses of that verb.

5. A term or word defined herein is meant to include both the lower and upper case reference to such term or word.

III. INSTRUCTIONS

1. You are requested to produce all documents in your possession, custody, or control that are described below. In so doing, please produce documents that are in the possession of your partners, officers, employees, attorneys, accountants, representatives, or agents, or that are otherwise subject to your custody or control.

2. Unless otherwise indicated, the documents to be produced include all documents prepared, sent, dated or received, or those that otherwise came into existence any time during the time period described herein.

3. The production by one person, party, or entity of a document does not relieve another person, party, or entity from the obligation to produce his, her, or its own copy of that document, even if the two documents are identical.

4. In producing documents, you are requested to produce a copy of each original document together with a copy of all non-identical copies and drafts of that document. If the original of any document cannot be located, a copy shall be produced in lieu thereof, and shall be legible and bound or stapled in the same manner as the original.

5. Documents shall be produced as they are kept in the usual course of business. All documents shall be produced with a copy of the file folder, envelope, or other container in which the documents are kept or maintained. All documents shall be produced intact in their original files, without disturbing the organization of documents employed during the conduct of the ordinary course of business and during the subsequent maintenance of the documents.

6. ESI shall be produced in accordance with the technical specifications set forth in parties' Stipulation and Order for The Production of Documents and ESI [Doc 449] which is attached as Appendix "A."

7. Documents not otherwise responsive to this production request shall be produced if such documents mention, discuss, refer to, or explain the documents which are called for by this production request, or if such documents are attached to documents called for by this production request and constitute routing slips, transmittal memoranda, or letters, comments, evaluations or similar materials.

8. Each document requested herein is requested to be produced in its entirety and without deletion or excisions, regardless of whether you consider the entire document to be relevant or responsive to this request.

9. If you intend to assert an objection to any request, you must nonetheless respond and produce any responsive documents or ESI that are not subject to the stated objection. If you intend to object to part of a request or category, you must specify the portion of the request to which you object, and must produce documents responsive to the remaining parts of the request.

10. If you intend to withhold documents or ESI otherwise discoverable under the Federal Rules of Civil Procedure by claiming that they are privileged or subject to protection as trial-preparation material, you will have to make that claim in accordance with Federal Rule of Civil Procedure 45(e)(2). As to any document or ESI to be withheld on privilege or work product grounds, you will also have to identify the author or originator, the addressees and/or recipients, the date, the nature of the document or ESI, the present custodian and location, and include a statement of the factual and legal reason(s) why the document or ESI is being withheld from production. Documents you designate as privileged material are to be produced in response to these requests. The provisions governing the production of "Privileged Material" as defined in the operative Protective Order submitted to the Court and that will govern this Action, will apply to documents produced in response to these requests. A copy of the Stipulated Protective Order [Doc 298] is attached hereto as Appendix "B".

11. If no document or ESI responsive to a request exists, please state that no responsive document or ESI exists.

12. Notwithstanding a claim that a document is protected from disclosure, any document so withheld must be produced with the portion claimed to be protected redacted at the time of any production.

13. These requests are continuing in nature and require supplemental response and continuous production.

V. RELEVANT TIME PERIOD

The relevant time period for each Document to Be Produced Request is for January 1, 2014 through the date of responses (the "Relevant Time Period"), unless otherwise specifically indicated, and shall include all documents and information that relate to such period, even though prepared or published outside of the relevant time period. If a document prepared before this period is necessary for a correct or complete understanding of any document covered by a request, you must produce the earlier or subsequent document as well. If any document is undated and the date of its preparation cannot be determined, the document shall be produced if otherwise responsive to the production request.

VI. DOCUMENTS TO BE PRODUCED

1. Documents sufficient to show the scope of services—if any—that you performed for Equifax in connection with Equifax's purchase, license, or implementation of Comcast Corporation, or any other company's, Computer System security software.

2. Documents sufficient to identify which of your products, software or services Equifax utilized, purchased, acquired, or licensed, the period of time the goods or services were utilized, the price(s) paid, as well as a copy of the contract or agreement applicable to the goods or services that were identified or involved in the Data Breach.

3. Any written report (including drafts) or other documentation that You provided to Equifax concerning the products, services, and work You provided or proposed to provide in connection with Equifax's Computer Systems, POS Technology, Security, and/or the Data Breach, including any vulnerability scan, penetration test, or risk assessment performed for any purpose, or any other evaluation, assessment, investigation, report concerning the disclosure of Customer Identifying Information, including Payment Card Data.

4. Documents sufficient to identify each of your Employees who consulted with or provided services to Equifax that were identified or involved in the Data Breach.

5. Documents relating to the level of security expertise at Equifax, including the IT and Security Departments, the Chief Information Security Officer.

6. All product documentation, including specifications, manuals, and user guides for any of your products or software applications that Equifax purchased, licensed, acquired, installed, or utilized on any Computer System that was identified or involved in the Data Breach.

7. A copy of any policies, protocols, recommendations, analysis, or training that Comcast Corporation provided to Equifax regarding data retention and/or the security of Equifax's Computer Systems or Computer Network.

8. A copy of documents sent to or received from Equifax concerning the installation, set up, configuration, specifications, upgrading, testing, monitoring, troubleshooting, or support of each of your products utilized, purchased, or licensed by Equifax, including Equifax's specifications for any Computer System identified or involved in the Data Breach.

9. Documents sufficient to show communications you sent to or received from Equifax or any third party concerning an assessment of the security or vulnerability of Equifax's Computer Systems.

10. Documents reporting and/or depicting unauthorized exfiltration of data from Equifax's computer systems.

11. Copies of all communication regarding the Data Breach, security of data, or security vulnerabilities with Equifax or any third party (including emails, IM's, voicemail and test messages).

12. Documents concerning your investigation regarding the Data Breach, including any documents provided in connection with any investigation involving the PCI standards.

13. All documents and testimony that you produced to or received from any government entity or law enforcement concerning its investigation of the Data Breach, as well as any documents reflecting that testimony.

14. Documents that you used or relied upon to prepare any response to any governmental entity or law enforcement inquiry into the Data Breach.

15. Documents that you provided to or received from Equifax related to its investigation of the Data Breach, including any documents which explain your involvement in the Data Breach.

16. Documents concerning each of the notices or alerts that Equifax should have or did receive from you or that were generated by your products, services or software in connection with the Data Breach, data security, or security vulnerabilities, including, but not limited to, the notices or alerts themselves.

17. Documents that you received from or provided to Equifax which describe the security measures, policies, and procedures for accessing Equifax's Computer Systems, including training materials and the scope of access rights for any Computer System identified or involved in the Data Breach.

18. Documents regarding any upgrades, modifications, or changes you recommended to Equifax.

19. Documents regarding any instructions you made to Equifax relating to the storage of personal information on Equifax's computer systems.

20. Documents regarding the Apache Struts CVE-2017-5638 vulnerability, Equifax's awareness of the vulnerability, and Equifax's efforts to identify affected websites and to respond to the vulnerability.

21. Documents reflecting the vulnerability in the Apache Struts web application framework and Equifax's attempt to patch the affected web application before bringing it back online.

22. Documents regarding the Equifax's awareness of the vulnerability in its Dispute Portal, and Equifax's efforts to identify affected websites and to respond to the vulnerability.

23. Documents regarding Equifax's awareness of, and response to, to the cross-site scripting vulnerabilities described in a September 12, 2017 ZDNet article found at http://www.zdnet.com/article/equifax-freeze-your-account-site-is-also-vulnerable-to-hacking and on the vulnerability-tracking website Open Bug Bounty (https://www.openbugbounty.org).

24. Documents regarding the forensic investigations performed relating to the Data Breach announced on September 7, 2017, including any forensic reports and all drafts of said reports, including any reports prepared by Mandiant.

25. Documents regarding the Equifax Dispute Portal and its relationship to the Data Breach.

26. Documents reflecting the suspicious network traffic Equifax's Security team observed on its dispute portal web application on July 29, 2017.

27. Documents reflecting Equifax's decision to take the affected web application offline on July 30, 2017.

28. Documents used in preparing the September 7, 2017 disclosure of the Data Breach by then CEO Richard Smith, including all communications, meeting minutes, and reports.

29. Documents regarding the disclosure of the Data Breach to executive officers.

30. Notifications that Equifax received from its automated computer system informing it that its network or computer system had been compromised.

31. Reports from Equifax's security analysts identifying weaknesses in Equifax's computer system and databases prior to the Data Breach.

32. Documents that identify individuals whose personal identifiable information was revealed in the Data Breach.

33. Documents relating to the 'long-term security improvements' identified by Equifax in its September 15, 2017 statement.

34. Documents relating to the 'short-term remediation steps' identified by Equifax in its September 15, 2017 statement.

35. Documents that identify all vendors that Equifax consulted with or retained to advise regarding the security of its databases and all personal identifiable information that Equifax stored.

36. Documents that describe the encryption Equifax utilized on its databases storing personal identifiable information.

37. Documents that Equifax prepared after the Data Breach and before announcing the breach to the public.

38. Reports reflecting audits of Equifax's computer network security.

39. Documents regarding Equifax's storage and protection of Customer Identifying Information, including Payment Card Data.

40. Documents that identify the activity logs, server hard drives and backups, traffic logs, access and entry logs, system event log data and any other data base log files relating to the Data Breach.

41. All captured network traffic for the attacker IP address identified during the Data Breach.

42. Documents relating to the detection, monitoring, and security of Equifax's computer systems and its practices to protect against cyber-attacks.

43. Documents regarding the use of Equifax employees using their Equifax email address to create accounts at sites unrelated to Equifax and its business.

44. Data reflecting the identification of Payment Cards that were subject to the Data Breach including the account number, original expiration date, card reissue dates and new expiration dates.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2800 1:17-md-2800-TWT ALL ACTIONS

STIPULATION AND ORDER FOR THE PRODUCTION OF DOCUMENTS AND ESI

This Stipulated Protocol for Producing Documents and ESI (the "ESI Protocol") shall govern the production of documents and electronically stored information ("ESI") by the parties in the above-captioned litigation.

The ESI Protocol shall govern productions made by any third party who is subpoenaed in this action unless otherwise agreed to by the issuing party and the third party. Accordingly, the ESI Protocol shall be attached to any subpoena issued in this action.

I. Production of Documents Originating as Paper

1. **TIFFs**. Documents should be produced as single-page, black and white, group IV TIFFs imaged at 300 dpi. Bates numbers, confidentiality designations (in accordance with the protective order governing the case), and redactions (to the extent they are necessary) should be burned into the image.

Original document orientation shall be maintained (*i.e.*, portrait to portrait and landscape to landscape) where reasonably possible. TIFF image files should be provided in an "Images" folder.

Documents containing color need not be produced in color. However, the parties will consider reasonable requests for reproduction of color document if an original document contains color necessary to understand the meaning or content of the document. Any documents produced in color should be produced in JPG format.

2. **Unitizing Documents**. In scanning paper documents, the parties will utilize logical unitization of documents such that distinct documents may not be merged into a single record, and single documents may not be split into multiple records (*i.e.*, paper documents should be logically unitized). For example, documents stored in a binder, folder, or similar container (each a "container") should be produced in the same order as they appear in the container. The front cover of the container should be produced immediately before the first document in the container. The back cover of the container should be produced immediately after the last document in the container. The parties will undertake reasonable efforts to, or have their vendors, logically unitize documents in accordance with the requirements of this paragraph, but

nothing in this paragraph shall require the parties to undertake efforts to unitize documents that would be unduly burdensome. The parties agree to meet and confer to address situations in which a party believes that documents have not been properly unitized.

3. **Parent-Child Relationships**. The parties shall undertake reasonable efforts to preserve parent-child relationships within a document family (the association between an attachment and its parent document). The child document(s) should be consecutively produced immediately after the parent document. The parties shall undertake reasonable efforts to produce each document with the production number for the first and last page of that document in the "BegBates" and "EndBates" fields of the data load file and with the "BegAttach" and "EndAttach" fields listing the production number for the first and last page in the document family. Nothing in this paragraph shall require the parties to undertake unduly burdensome efforts to preserve parent-child relationships within a document family for hard copy documents. The parties agree to meet and confer to address situations in which a party believes that parent-child relationships have not been adequately preserved.

4. **Optical Character Recognition**. The producing party shall provide optical character recognition ("OCR") text files for all documents

originating as paper. Text files should be in Unicode [UTF-8] format. All references below to 'Unicode' are synonymous with UTF-8. To the extent that documents have been run through OCR software, the full text shall be provided on a document-level in an appropriately formatted text file (.txt) that is named to match the first bates number of the document. Text files should be provided in a "Text" folder. To the extent that a document is redacted, the text files should not contain the text of the redacted portions.

5. **Unique IDs**. Each TIFF image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be zero-padded (*e.g.*, ABC000000001). A single prefix with a fixed width should be used for each producing party, along with a fixed-width numerical portion. If a Bates number or set of Bates numbers is skipped in a production, the producing party will so note in a cover letter or production log accompanying the production. Bates numbers will be unique across the entire production and prefixes will be consistent across all documents a party produces in the litigation.

6. **Data Load Files**. Documents shall be provided with: (a) a delimited data file (.dat, .csv, or .txt) [Unicode]; and (b) an image load file (.lfp, .opt, or .dii), as detailed in Appendix 1.

II. Production of ESI

8. **TIFFs**. Documents should be produced as single-page, black and white, group IV TIFFs imaged at 300 dpi. Whenever it is practical to do so, the document's original orientation should be maintained (*i.e.*, portrait to portrait and landscape to landscape). Bates numbers, confidentiality designations (in accordance with the protective order governing the case), and redactions (to the extent they are necessary) should be burned into the image. TIFF image files should be provided in an "Images" folder.

9. **Extracted Text Files**. For each document, a single Unicode text file shall be provided along with the image files and metadata. The text file name shall be the same as the Bates number of the first page of the document. File names shall not have any special characters or embedded spaces. Electronic text must be extracted directly from the native electronic file to the extent reasonably available unless the document is an image file or contains redactions. In these instances a text file created using OCR should be produced in lieu of extracted text.

10. **Unique IDs**. Each image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be zero-padded (*e.g.*, ABC-000001), taking into

consideration the estimated number of pages to be produced. If a Bates number or set of Bates numbers is skipped in a production, the producing party will so note in a cover letter or production log accompanying the production. Bates numbers will be unique across the entire production and prefixes will be consistent across all documents a party produces in the litigation.

11. **Parent-Child Relationships**. The relationship between attachments, enclosures, embedded files, and/or exhibits to any parent document shall be preserved. The child-document should be consecutively produced immediately after the parent-document. Each document shall be produced with the production number for the first and last page of that document in the "BegBates" and "EndBates" fields of the data load file and with the "BegAttach" and "EndAttach" fields listing the production number for the first and last page in the document family.

12. **Native Format**. Excels, PowerPoints, delimited text files, audio files, video files, and additional documents of a type which cannot be reasonably converted to useful Tiff images shall be produced as native files along with extracted text and metadata identified in Appendix 2. Natively produced documents should include a Bates-numbered TIFF image placeholder stating that the document has been produced in native format.

13. The requesting party may ask for certain other documents and/or databases initially produced in TIFF format to be produced in their native format in the event that the TIFF format is not reasonably usable. The requesting party shall identify the documents by their Bates numbers and the documents should be produced in their unaltered native format, provided, however, that the producing party shall not be required, absent extraordinary circumstances, to produce any redacted files in native format.

14. To the extent that the information in a native file must be redacted, the producing party may produce TIFF images with burned in redactions in lieu of a native file and TIFF placeholder image. The producing party shall make reasonable efforts to ensure redacted TIFF images of native files are legible and usable. If redacting TIFF images and to the extent that any of the following can be automated, the producing party, or its e-discovery vendor, should make reasonable efforts to: (1) reveal hidden rows, columns, or sheets prior to converting the document to TIFF; (2) clear any filters that may conceal information; (3) adjust column widths and row heights to avoid numbers or other text content being truncated or appearing as "########"; (4) ensure that column and row headings print; (5) ensure that the tab name appears in the header or footer of the document; (6) process comments so that they are

produced at the end of the spreadsheet; and (7) process spreadsheets so that they print across then down. If good cause exists, requesting party may ask the producing party to manually undertake the foregoing for certain documents identified by Bates number by the requesting party to the extent the document was originally produced with concealed information. The producing party shall not unreasonably deny such a request.

15. **Request for Native Files**. Other than the file types referenced in paragraph 12 above, a producing party need not produce documents in native format. If good cause exists for the receiving party to request production of certain documents in native format, the receiving party may request production in native format by providing (1) a list of the Bates numbers of documents it requests to be produced in native format; and (2) an explanation of the need for reviewing such documents in native format. The producing party shall not unreasonably deny such requests. In the event the producing party agrees to produce documents in native format, the producing party shall produce an overlay to ensure that the "NativeLink" entry in the data load file indicates the relative file path to each native file in such production, and all extracted text and applicable metadata fields set forth in Appendix 2. Documents and overlays shall be produced within 21 days of the request unless the request is reasonably

denied or the parties agree to a different time. The parties shall meet and confer concerning any request for native files before seeking Court intervention. In the event the Court orders a producing party to produce documents in native format, documents and overlays shall be produced within 14 days of the order or such other time as the Court may order.

16. **Tracked Changes and Comments**. To the extent that a document contains tracked changes or comments, the document should be imaged showing tracked changes and comments.

17. **Password Protected Files**. The producing party shall produce passwords for any password-protected files to the extent the passwords are reasonably available.

18. **Embedded Documents.** If reasonably possible, embedded ESI documents (*e.g.* a spreadsheet embedded within a word processing document) will be extracted, produced as independent document records and related back to the respective top level parent document (*e.g.*, standalone file, email message, *etc*.) via the BegAttach and EndAttach fields referenced in Appendix 2. Related documents will be produced within a continuous Bates range. Nothing in this paragraph will require a party to extract or produce information from an embedded or attached internet link.

19. **Data Load Files**. Documents shall be provided with: (a) a delimited data file (.dat, .csv, or .txt) [Unicode] and (b) an image load file (.lfp, .opt, or .dii) as detailed in Appendix 1. Nothing in this Order will limit the parties from discussing load file changes throughout the course of the litigation.

20. **Metadata**. Appendix 2 sets forth the metadata fields that must be produced to the extent that metadata exists for a particular document subject to the limitations discussed below. To the extent that metadata does not exist, is not reasonably accessible or available, or would be unduly burdensome to collect, nothing in this ESI Protocol shall require any party to extract, capture, collect or produce such data. The parties are not obligated to populate manually any metadata fields except those fields marked with an "X" in the "Must Be Populated" field in Appendix 2, provided that the metadata exists, is reasonably accessible or available, and would not be unduly burdensome to collect.

21. **Deduplication**. Documents should be deduplicated at the family-group level provided that the producing party identifies the additional custodians in an Additional Custodian field. A party may also de-duplicate "near-duplicate" email threads as follows: in an email thread, only the final-in-time document need be produced, assuming that all previous emails in the thread are contained within the final message and provided that the software used to identify these

"near- duplicate" threads is able to identify any substantive differences to the thread such as changes in recipients (*e.g.*, side threads, subject line changes), selective deletion of previous thread content by sender, *etc*. Where a prior email contains an attachment, that email and attachment shall not be removed as a "near-duplicate."

III. Production of Databases and Other Structured Data

22. The parties shall meet and confer prior to the production of reasonably accessible structured data ESI to ensure such ESI is produced in a reasonable, proportional, mutually agreeable, and reasonably useable format.

IV. Processing of Third-Party Documents

23. A party that issues a non-party subpoena ("Issuing Party") shall include a copy of this ESI Protocol as an attachment to the subpoena and request that the non-party produce documents in accordance with the specifications set forth herein.

24. The Issuing Party may request that the non-party simultaneously produce documents to the Issuing Party and all other parties. If the non-party produces documents only to the Issuing Party, to the extent practical given the data volume, productions by a non-party should be produced by the Issuing Party to all other parties within seven days.

25. Nothing in this ESI Protocol is intended to or should be interpreted as narrowing, expanding, or otherwise affecting the rights of the parties or non-parties to object to a subpoena.

V. Miscellaneous Provisions

26. The following specifications govern the production of all documents regardless of source, unless otherwise noted in this ESI Protocol:

27. **Custodian or Originating Source**. The custodian or originating source shall be identified in the Custodian field of the database load files. Documents found in the possession of a natural person (or on a natural person's hardware or storage media) should be produced in such fashion as to identify the natural person. Documents found in the possession of a department, group, entity, or other common facility (*e.g.*, office, file room, archive, network storage, file share, back-up, hard drive, *etc*.) should be produced in such a fashion as to identify the department, group, entity, or facility. A producing party shall use a uniform description of a particular custodian across productions.

28. **Foreign Language**. Foreign language text files and metadata should be delivered with the correct encoding to enable the preservation of the documents' original language.

29. **Dates**. All documents shall be processed so as to show the date and time in UTC or Eastern Standard Time.

30. **Search Terms and Technology Assisted Review**. The parties have begun to meet and confer as directed by the Court relating to the process of searching for documents responsive to discovery, including, specifically, the identification of any search terms and custodians to the extent they are necessary in responding to specific discovery requests. The Court expects that the parties will continue to meet and confer on this issue as necessary to ensure that discoverable, responsive, non-privileged documents are identified and produced as efficiently as possible. In addition, the parties are directed to meet and confer with regard to any proposed use of technology assisted review ("TAR") and the terms of any additional case management orders that may be needed to address issues relating to searches of electronically stored information.

31. **Production Media**. The preferred means of producing documents is via secure FTP or secure file share. However, documents may also be produced via CD, DVD, flash drive, or hard drive if (a) the size of the production exceeds the size limitations applicable to the producing party's secure FTP or file share or (b) if the interest of preserving the confidentiality of the information produced outweighs the speed and efficiency of producing documents via secure

FTP or secure file share. To the extent possible, physical media should be write protected before it is produced.

32. **Naming Convention for Production Media**. Whether produced via secure FTP, file share, or physical media, the files produced should be combined into a compressed file such as .zip, .rar, *etc*. The compressed file should be named so as to indicate the producing party, the date of the production, and the sequence of the production (*e.g.*, "Equifax Production 20180508-001"). If the production is made using physical media, the media should be labeled to include (a) text referencing that it was produced in *In re: Equifax, Inc. Customer Data Security Breach Litigation*, MDL DOCKET NO. 2800 1:17-md-2800-TWT; (b) the Bates Number range of the materials contained on the media; (c) and the filename(s) of the compressed file(s) contained on the media such as the example included above.

33. **Replacement Productions**. Any replacement production will be transmitted with a cover letter or email to identify the production as a replacement and cross-reference the BegBates and EndBates of the documents being replaced. If the replacement production is being transmitted by physical media, the media shall include the phrase "Replacement Production."

34. **Inability to Produce Metadata**. If the producing party is unable to produce metadata for a particular field, it will provide an explanation of that inability if requested by the receiving party.

35. **Encrypted Data**. To the extent data is encrypted before it is produced, the producing party shall contemporaneously transmit the credentials necessary to decrypt the data.

36. **Non-Waiver**. Nothing in this ESI Protocol shall be interpreted to require disclosure of irrelevant information or relevant information protected by the attorney-client privilege, work-product doctrine, or any other applicable privilege or immunity. The parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of documents.

37. **Protective Order**. All productions are subject to the Protective Order entered by the Court in this Action.

38. **Good Faith Resolution of Disputes**. The parties shall make good faith efforts to comply with and resolve any differences concerning compliance with this ESI Protocol. If a producing party, notwithstanding their good faith efforts, cannot comply with any material aspect of this ESI Protocol or if compliance with such material aspect would be unreasonable, such party shall inform the requesting party in writing a reasonable time before the date of

production as to why compliance with the ESI Protocol is impossible or unreasonable. No party may seek relief from the Court concerning compliance with the ESI Protocol unless it has conferred in good faith with the affected parties.

DATED: August 9, 2018

/s Kenneth S. Canfield
Kenneth S. Canfield
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E.
Suite 1600
Atlanta, Georgia 30309

Amy E. Keller
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112

Consumer Plaintiffs' Co-Lead Counsel

Roy E. Barnes
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060

/s S. Stewart Haskins II
KING & SPALDING LLP
David L. Balser
Georgia Bar No. 035835
Phyllis B. Sumner
Georgia Bar No. 692165
S. Stewart Haskins II
Georgia Bar No. 336104
Elizabeth D. Adler
Georgia Bar No. 558185
John C. Toro
Georgia Bar No. 175145
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
psumner@kslaw.com
shaskins@kslaw.com
eadler@kslaw.com
jtoro@kslaw.com

Counsel for Equifax Inc.

David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350

Consumer Plaintiffs' Co-Liaison Counsel

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500
Washington, DC 20005

Eric H. Gibbs
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, DC 20006

Ariana J. Tadler
MILBERG TADLER PHILLIPS GROSSMAN LLP
One Penn Plaza
19th Floor
New York, New York 10119

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064

Consumer Plaintiffs' Steering Committee

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, GA, 30303

Consumer Plaintiffs' State Court Coordinating Counsel

/s Joseph P. Guglielmo

Joseph P. Guglielmo
SCOTT+SCOTT ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169

Gary F. Lynch
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222

Financial Institution Plaintiffs' Co-Lead Counsel

Craig A. Gillen
GILLEN WITHERS & LAKE, LLC
3490 Piedmont Road, N.E.
One Securities Centre, Suite 1050
Atlanta, GA 30305

MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305

Ranse Partin
CONLEY GRIGGS PARTIN LLP
4200 Northside Parkway
Building One, Suite 300
Atlanta, Georgia 30327

Financial Institution Plaintiffs' Co-Liaison Counsel

Arthur M. Murray
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130

Stacey P. Slaughter
ROBINS KAPLAN LLP
800 LaSalle Avenue Suite 2800
Minneapolis, MN 612-349-8500

Charles H. Van Horn
BERMAN FINK VANHORN P.C.
3475 Piedmont Road, Suite 1100
Atlanta, GA 30305

Allen Carney
CARNEY BATES & PULLIAM, PLLC

519 W. 7th Street
Little Rock, AR 72201

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North
Suite 300
Minneapolis, MN 55401

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401

Karen S. Halbert
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223

Brian C. Gudmundson
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402

Financial Institution Plaintiffs' Steering Committee

IT IS SO ORDERED.

Date: August 10, 2018

/s/Thomas W. Thrash
Thomas W. Thrash
United States District Judge

APPENDIX 1: PRODUCTION MEDIA AND LOAD FILE FORMATS

Production Media

- The Producing Party shall produce documents on readily accessible, computer or electronic media including CD-ROM, DVD, external hard drive (with standard PC compatible interface or access to a secure Online Repository agreed upon by the parties) or via secure FTP site. Each piece of Production Media shall be assigned a production number or other unique identifying label corresponding to the date of the production of documents on the Production Media. The Producing Party shall accompany all document productions with a transmittal cover letter identifying by Bates Number the documents produced.

Image Load Files

- Production image load files shall have all corresponding images logically grouped together;
- Production volumes should only include one image load file per production volume;

- The name of the image load file shall mirror the name of the delivery volume, and should have an .lfp, .opt or .dii[1] extension (*e.g.*, ABC001.lfp);
- The volume names shall be consecutive (*i.e.*, ABC001, ABC002, *et seq*.);
- The load file shall contain one row per TIFF or JPG image;
- Every image in the delivery volume shall be contained in the image load file;
- The image key shall be named the same as the Bates number of the page;
- Load files shall ***not*** span across media (*e.g.*, CDs, DVDs, hard drives, *etc*.), *i.e.*, a separate volume shall be created for each piece of media delivered.

Metadata Load Files

- The metadata load file shall use the following delimiters:
  - Column Delimiter: ASCII character (020)
  - Text Qualifier: þ ASCII character (254);
  - New line: Registered sign - ® (ASCII 174).
- Data for documents shall be produced in only one data load file throughout the productions, unless that document is clearly noted as being a replacement document or if supplemental custodian information is provided;
- The first line shall contain the field names in the order of the data set forth in Appendix 2;

[1] If a .dii file is produced, the accompanying metadata load file shall be separate from the .dii file and not contained within the .dii file itself.

- Metadata fields that are not applicable to a document shall still be populated in the data load file with Empty Quotes, eg |^^|^^, *etc*;
- A carriage-return line-feed shall be used to indicate the start of the next record;
- Load files shall ***not*** span across media (*e.g.*, CDs, DVDs, hard drives, *etc*.); a separate volume shall be created for each piece of media delivered;
- The name of the metadata load file shall mirror the name of the delivery volume, and shall have a .dat, .csv or .txt extension (*i.e.*, ABC001.dat);

The volume names shall be consecutive (*i.e.*, ABC001, ABC002, *et seq.*).

Appendix 2

ESI Metadata and Coding Fields

Field	Description	Must Be Populated
BegBates	Beginning Bates number of the document	X
EndBates	Ending Bates number of the document	X
BegAttach	Beginning Bates number of the attached documents	X
EndAttach	Ending Bates number of the attached documents	X
AttachRange	Bates number of the first page of the parent document to the bates number of the last page of the last attachment "child" document	X
Page Count	Total number of pages in the document	X
Attachment Count	Indicates the number of attachments to the parent document	X
Custodian	Natural person, group, department, entity, *etc*. in whose possession the document was found Custodian names, including those listed within the "Additional Custodian" field, should be uniform and unambiguous per Custodian.	X
Additional Custodian	Other natural person(s), group(s), department(s), entity(ies), *etc*. in whose possession the document was found if duplicate versions of the document are not produced	X
File Size	Size in kilobytes (KB) of the document	X
NativeLink	Relative file path to each native document in the production (This field will be produced with all native ESI).	
TextPath	The relative path to the corresponding OCR or extracted text file included with a production volume	X
Hash Value	MD5 or SHA-1 Hash value, unique document identifier	X
Confidential	"Confidential" to indicate that the document has been designated Confidential. "Highly Confidential" to indicate that the document has been designated Highly Confidential. Otherwise, this field should be null.	X
Redacted	Yes or No indication of whether the document at issue is redacted.	X

Field	Description	Must Be Populated
Author	Author field extracted from the metadata of the native file	X
From	Email sender	X
Agent ID	If the item was created by someone on behalf of the email account owner, ID of the agent who created/sent the item	
To	Person to whom an email is addressed	X
CC	Recipient(s) of "carbon copies" of the email message	X
BCC	Recipient(s) of "blind carbon copies" of the email message	X
Subject	Subject field extracted from the metadata of the native file	X
Date Sent	Date the email message was sent (produced in MM/DD/YYYY format)	X
Time Sent	Time the email message was sent (produced in HH:MM AM/PM	X
Importance	For emails, "High," "Low," or "Normal" (or equivalent if an email client other than Outlook was used); Null if no value selected	X
Sensitivity	For Outlook (or equivalent) emails, "Normal," "Private," "Personal," or "Confidential"; Null if no value selected	
Follow Up Flag	System data; Null if no status	
Read Status	Read or Unread	
Has Attachments	Indicates that an email has attachments	X
Email Folder Path	The original email folder	
File Type	Email, attachment, individual file, paper, *etc*.	X
File Extension	File extension of document (.msg, .doc, .xls, *etc*.)	X
File Name	Name of original file	X
Original Path	The original file path for non-email ESI	

Field	Description	Must Be Populated
Title	Title of a non-email document (Microsoft Title field)	X
Date Created	For non-emails (produced in MM/DD/YYYY format)	X
Time Created	For non-emails (produced in HH:MM AM/PM format)	X
Date Last Modified	For non-emails (produced in MM/DD/YYYY format)	X
Time Last Modified	For non-emails (produced in HH:MM AM/PM format)	X
Date Last Accessed	For non-emails (produced in MM/DD/YYY format)	X
Time Last Accessed	For non-emails (produced as HH:MM AM/PM	X
Last Modified By	Person who last modified a document	X
Track Changes	"Yes" to indicate that the document includes tracked changes. Otherwise, this field should be null.	X
Marginalia	For hard-copy documents, yes or no indication of whether the document at issue contains handwritten notations, notes, or marginalia	

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE EQUIFAX, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	MDL DOCKET NO. 2800 1:17-md-2800-TWT ALL ACTIONS

STIPULATED PROTECTIVE ORDER

I. PURPOSES AND LIMITATIONS

Disclosure and discovery activity in this action may involve production of confidential, proprietary, or private information for which special protection from public disclosure and from use for any purpose other than prosecuting this litigation may be warranted. The information likely to be the subject of the disclosure and discovery activity in this action also may involve unique risks related to privacy, data security, data governance, and data management that will be greater than in most cases. Accordingly, the parties hereby stipulate to and petition the Court to enter the following Stipulated Protective Order. The parties acknowledge that this Order does not confer blanket protections on all disclosures or responses to discovery and that the protection it affords from public disclosure

and use extends only to the limited information or items that are entitled to confidential treatment under the applicable legal principles.

II. DEFINITIONS

A. "**Appointed Counsel**" means those attorneys appointed by the Court to lead the litigation on behalf of the plaintiffs in the consumer and financial tracks (i.e., lead counsel, liaison counsel, and steering committee members, and the attorneys and staff at their firms), and counsel of record for Defendant Equifax, Inc. and their firms.

B. "**Confidential Information**" means information:

1. that may reveal a trade secret or other confidential research, development, financial, data security information, network security details and diagrams;

2. that may reveal information that is not commonly known by or available to the public and derives value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain value from its disclosure or use;

3. that contains information that reveals personally identifiable information, as defined below, or personal or private financial information (collectively "Sensitive Information");

4. the disclosure of which is reasonably likely to result in unauthorized access of Sensitive Information; or

5. any other material that is confidential pursuant to applicable law.

C. "**Highly Confidential Information**" means a subset of extremely sensitive "Confidential Information," such as Sensitive Information, corporate network security details and other security information, competitively sensitive financial information, or any other information the disclosure of which to another party or non-party would create a substantial risk of serious harm that could not be avoided by less restrictive means.

D. "**Personally Identifiable Information" (PII),** for purposes of this Order, includes, but is not limited to: payment card numbers, financial account numbers, social security numbers, addresses, phone numbers, e-mail addresses, driver's license numbers or other state identification numbers, employer identification numbers, tax identification numbers, passport numbers, or a foreign government equivalent of any of these numbers or identifiers.

The parties recognize that other personal data (*e.g.*, name, citizenship, birth date, spousal and familial information), particularly in combination with one another, may reveal sensitive PII and, for purposes of this Order, PII also includes such data when in combination with any other Sensitive Information.

E. **"Producing Party" or "Designating Party"** means the party or third party that produced the Protected Material.

F. **"Privileged Material"** means any document or information that is, or that the Producing Party asserts is, protected from disclosure by a privilege or other immunity from discovery, including, without limitation, the attorney-client privilege, the work product immunity, or the joint defense or common interest privilege.

G. **"Protected Material"** means any document or information which has been designated as "Confidential" or "Highly Confidential" pursuant to this Protective Order. Documents that quote, summarize, or contain Confidential Information or Highly Confidential Information (*e.g.*, discovery responses, transcripts, and court filings) may be accorded status as Protected Material, but, to the extent reasonably feasible, shall be prepared in such a manner that the Confidential Information or Highly Confidential Information is provided separately from that not entitled to protection.

III. DESIGNATING PROTECTED MATERIAL

A. The Producing Party has an obligation to stamp documents "Confidential" or "Highly Confidential" in good faith and must take care to limit any such designation to specific material that qualifies under the appropriate standards. The Parties shall make Confidential and Highly Confidential designations in good faith to ensure that only those documents or testimony that

merit Confidential or Highly Confidential treatments are so designated. Either designation may be withdrawn by the designating Party.

B. The Producing Party must designate for protection only those parts of material, documents, items, or oral or written communications that qualify – so that other portions of the material, documents, items, or communications for which protection is not warranted are not swept unjustifiably within the ambit of this Order. Mass, indiscriminate, or routinized designations are prohibited. If it comes to a Producing Party's attention that information or items that it designated for protection do not qualify for protection at all, or do not qualify for the level of production initially asserted, that Producing Party must promptly notify all other Parties that it is withdrawing the mistaken designation.

C. Third parties producing documents in the course of this action may also designate documents as "Confidential" or "Highly Confidential" subject to the same protections, obligations, and constraints as the parties to the action. A copy of this Protective Order shall be served along with any subpoena or document request served on third parties in connection with this action. All documents produced by such third parties shall be treated as "Highly Confidential" for a period of 14 days from the date of their receipt, and during that period any party or the third party

may designate such documents as "Confidential" or "Highly Confidential" pursuant to the terms of the Protective Order.

IV. SCOPE

A. The protections conferred by this Stipulation and Order cover not only Protected Material, but also (1) any information copied or extracted from Protected Material; (2) all copies, derivations, abstracts, excerpts, summaries, or compilations of Protected Material; and (3) any testimony, conversations or presentations by parties or their counsel that might reveal Protected Material.

B. However, the protections conferred by this Stipulation and Order do not cover the following information: (1) any information that is in the public domain at the time of disclosure to a receiving party or becomes part of the public domain after its disclosure to a receiving party as a result of publication not involving a violation of this Order, including becoming part of the public record through trial or otherwise; and (2) any information known to the receiving party prior to the disclosure or obtained by the receiving party after the disclosure from a source who obtained the information lawfully and under no obligation of confidentiality to the Designating Party.

C. Any use of Protected Material at trial shall be governed by a separate agreement or order.

D. Nothing in this Protective Order diminishes the protections afforded to sensitive information by this Court's Standing Order No. 04-02. The Court has instructed the Parties that documents to be filed in this MDL are presumptively public, and handling of Protected Material, including sealed filing of such materials, imposes a burden upon the Court. Accordingly, the Parties shall only designate as "Confidential" or "Highly Confidential" information that is confidential under applicable law. The Court shall require an appropriate showing in order to justify any claim of confidentiality under existing law.

E. The Court and the parties recognize that plaintiffs have alleged they were the victims of a data breach that exposed their Sensitive Information and, as a result, allege that they face a risk of future harm, including the alleged risk of future fraud and/or identity theft. Thus, the parties will exercise particular caution before publicly filing personal or financial information.

V. NON-DISCLOSURE OF PROTECTED MATERIAL

A. Except with the prior written consent of the Producing Party, as provided in this Order, or as may be subsequently ordered by the Court, Protected Material may not be disclosed by a non-Producing Party to any person except as described below.

B. Protected Material may be disclosed by a non-Producing Party only to:

1. The parties, their officers, directors, and employees only to the extent reasonably necessary to provide assistance with the litigation, and Appointed Counsel for the parties in all cases in MDL 2800, including the in-house lawyers of such parties and the partners, associates, contract attorneys, secretaries, paralegal assistants, and employees of such counsel, only to the extent reasonably necessary to render professional services in the litigation, and for use exclusively in these actions (and for no other purpose). "Parties" include named plaintiffs, class representatives and proposed class representatives. No Stamped Confidential Documents may be disclosed to putative class members other than the named plaintiffs, class representatives and proposed class representatives;

2. Judges, the jury, court reporters, court personnel, and videographers present at trial, hearings, arguments, depositions and any other judicial proceedings held in this litigation;

3. Persons shown on the face of the document to have authored or received it;

4. Other persons who may be designated by written consent of the Producing Party or pursuant to Court order, but only for purposes of this litigation and for no other purpose;

5. Witnesses during depositions and trial, who have previously been asked to sign the Acknowledgment of Confidentiality Designations and Agreement To Be Bound by Terms of Court Order attached as Exhibit A (the "Acknowledgement");

6. Persons noticed for depositions or designated as trial witnesses, to the extent reasonably necessary to prepare such persons to testify, who have previously been asked to sign the Acknowledgment;

7. Consultants or experts retained for the purpose of assisting Appointed Counsel in this litigation who have previously executed the Acknowledgment and who are not current employees of a competitor of a party and have not, at the time of retention, agreed to become an employee of a competitor of a party; and

8. Third-party contractors retained for the purpose of organizing, filing, coding, converting, storing, or retrieving data or designing database programs for handling Protected Material who have previously executed the Acknowledgment.

C. Protected Material designated as "Highly Confidential" may be disclosed by a non-Producing Party only to:

1. Persons designated in paragraphs B(2)-(8), as well as Appointed Counsel, and the in-house lawyers of such parties and the partners, associates, contract attorneys, secretaries, paralegal assistants, and employees of such counsel, to the extent reasonably necessary to render professional services in the litigation.

2. Persons designated in paragraph B.1, not otherwise included in C.1., after they have signed the Acknowledgement and only to the extent it is reasonably necessary to prosecute their claims.

D. Counsel for all persons receiving Confidential Information in accordance with paragraphs (B)(5)-(B)(8) shall be responsible for obtaining, prior to disclosure and as a condition thereof, an Acknowledgment executed by the person to whom the counsel discloses the Confidential Information. Each non-party witness to whom Confidential or Highly Confidential Information is disclosed shall be advised that the Court has entered a Protective Order to limit

disclosure of Confidential and Highly Confidential Information, be provided a copy of the Protective Order, and be asked to sign the Acknowledgment. If a non-party witness has refused to sign the Acknowledgment, advising the witness of the matters in the immediately preceding sentence on the record shall serve as a substitute for the signing of the Acknowledgment and shall permit examination of the witness regarding documents or other information containing Confidential or Highly Confidential Information. Notwithstanding a witness's refusal to sign the Acknowledgment, any Confidential or Highly Confidential Information disclosed to the witness and any discussion of that information at the deposition shall maintain their confidential status.

E. A recipient of Protected Material shall keep the material in a secure area and shall exercise due care to restrict access to those persons described above. Any copies, excerpts, or compilations of Protected Material, whether in oral or written form, shall be subject to this Order to the same extent as the Protected Material itself, and, if in written form, must be labeled as Confidential or Highly Confidential. A recipient shall not duplicate any Protected Material except for use as working copies and for filing in court.

VI. DE-DESIGNATION AND CHALLENGING OF PROTECTED MATERIAL

A. Any party may request a change in the designation of any information designated as "Confidential" or "Highly Confidential." Any Protected Material shall be treated as designated until the change is completed. If the requested change in designation is not agreed to, the party asserting that the material is Confidential shall have the burden of proving that the information in question is within the scope of protection afforded by Fed. R. Civ. P. 26(c) and this Order.

B. Any party or non-party may challenge a designation of confidentiality at any time. Unless a prompt challenge to a Designating Party's confidentiality designation is necessary to avoid foreseeable, substantial fairness, unnecessary economic burdens or a significant disruption or delay of the litigation, a party does not waive its right to challenge a confidentiality designation by electing not to mount a challenge promptly after the original designation is disclosed.

C. The party challenging a confidentiality designation shall identify each challenged document by Bates number or otherwise specifically describe the document challenged and set forth the specific reasons why it does not believe the confidentiality designation is appropriate.

D. Within 21 days of a challenge to a designation, the party asserting confidentiality must move the Court for relief. Counsel for each party shall meet

and confer within seven days of a challenge to limit the scope of any issues requiring resolution by the Court. To that end, the parties shall identify exemplar documents for the Court's review, a ruling on which will allow the parties to resolve their disputes concerning any similar documents for which a confidentiality designation has been challenged.

VII. CONFIDENTIAL AND HIGHLY CONFIDENTIAL INFORMATION IN DEPOSITIONS

A. If a party, the current employee of a party, or anyone represented by counsel for a party, is noticed for deposition, that party's counsel is responsible for providing a copy of this Order to the witness and obtaining the witness's signature on the Acknowledgment prior to the deposition. If a non-party is subpoenaed for deposition, the counsel issuing the subpoena is responsible for providing a copy of this Order to the witness and attempting to obtain a signed Acknowledgment.

B. Parties and deponents may, within 30 days after receiving the deposition transcript from the court reporter, designate pages and lines of the transcript (and exhibits thereto) as Confidential or Highly Confidential by underlining or otherwise designating the portions of the pages that are confidential. (Documents marked as deposition exhibits that have been previously designated for protection under this Order do not need to be re-designated in order to maintain their designation.) The parties and the court reporter shall thereafter mark such

pages in all copies of the transcript with the legend, "CONFIDENTIAL — SUBJECT TO PROTECTIVE ORDER" or "HIGHLY CONFIDENTIAL — SUBJECT TO PROTECTIVE ORDER" and will note on the cover page of any such deposition the following legend: "Certain Designated Pages of this Deposition are Confidential and Subject to a Protective Order." Until expiration of the 30-day period, the entire deposition transcript will be treated as Highly Confidential pursuant to this Protective Order.

VIII. SUBPOENAS OR LEGAL PROCESS CALLING FOR DISCLOSURE OF PROTECTED MATERIAL

If a party receives a subpoena or other legal process which calls for disclosure of any Protected Material designated as Confidential or Highly Confidential by another party, then the party from whom disclosure is sought shall give prompt written notice (including a copy of such subpoena or other legal process) to counsel for the Designating Party, and shall not, to the extent permitted by applicable law, provide or otherwise disclose such documents or information until 21 days after providing notice to the Designating Party.

IX. FILING AND USE OF PROTECTED MATERIAL FOR PRETRIAL PURPOSES

A. Any document, material or other information entitled to protection under this Order that is submitted to the Court in support of a pleading, or

introduced at a hearing, trial or other proceeding in this action must be designated as "PROVISIONALLY SEALED" and electronically filed in the CM/ECF electronic filing system as a "Provisionally Sealed" pleading in accordance with the following process:

1. Provisionally Sealed filings can only be made during the Court's normal business hours of 9:00 A.M. to 4:30 P.M. (EST). Provisionally Sealed filings cannot be made when the Court is closed.

2. Before the anticipated filing of a Provisionally Sealed document, and no later than one day prior to the filing, counsel responsible for submitting the electronic filing must contact one of the following individuals by telephone to receive clearance by advising that a party intends to submit a filing that should be designated by the Clerk as a Provisionally Sealed document, identifying the name of the CM/ECF filer, and disclosing the date such filing will be made:

    a. Margaret Callier: (404) 215-1675

    b. Denza Bankhead: (404) 215-1662

    c. Darrell Satterfield: (404) 215-1682

3. Counsel filing such information must affirmatively indicate in the appropriate CM/ECF menu system prompt that the filing is being submitted as a Provisionally Sealed pleading by first designating the filing as "Under Seal" and then following the remaining menu prompts to designate the filing as Provisionally Sealed.

4. All such filings shall bear a legend on the cover page and in the header of each page indicating that they are being designated as PROVISIONALLY SEALED under this order.

Any documents submitted to the Court as Provisionally Sealed will not be available for public viewing. These documents shall only be available for viewing by Court personnel and Appointed Counsel for the parties and shall be subject to the restrictions on Confidential and Highly Confidential documents under this order, as applicable. If a filing designated as "PROVISIONALLY SEALED" is submitted to the Court in support of a pleading, the filing party shall serve the document containing the information designated as Confidential or Highly Confidential on counsel for the opposing party. Such information shall maintain its Provisionally Sealed status for ten business days. During this ten-day period, the party asserting confidentiality may move the Court to continue the protected status of the information by submitting to the Court a motion for continued protection. The time period for this motion may be extended by agreement of the parties or by leave of Court. A copy of the motion must be delivered to chambers (or to a Special Master duly appointed by the Court to review such materials) and accompanied with appropriate markings to identify the text, materials or information for which continued protection is warranted. The motion for continued protection shall set forth the reasons why the information should not be disclosed in a public filing. Once a motion has been filed for continued protection, the filing shall retain its Provisionally Sealed status until the Court or Special Master rules

on the motion. Should the Court appoint a Special Master to review such materials, the cost of the Special Master shall be borne by the party seeking to continue the protected status of the materials. If the Designating Party does not timely file such a motion for continued protection, the Designating Party will be deemed to have waived its confidentiality designations for the Confidential or Highly Confidential information contained in the filed document, and the Provisionally Sealed status will be removed and the document will be available to the public. In the event the Court continues protection of Provisionally Sealed documents, such documents will be viewable only by Court personnel and Appointed Counsel for the parties and shall remain subject to the restrictions applicable to Confidential and Highly Confidential documents under this order, as applicable.

B. Confidential or Highly Confidential material that contains Sensitive Information, or the disclosure of which is reasonably likely to result in unauthorized access of Sensitive Information, shall presumptively be entitled to continued protection until such time as determined otherwise by the Court.

C. The parties are instructed to use their best efforts to limit the filing of Confidential or Highly Confidential material under seal to those situations where such filing is necessary to the resolution of a motion or other matter before the

Court. Filing Confidential or Highly Confidential material under seal imposes a burden on the Court and should be avoided wherever possible.

D. A party who seeks to introduce protected information at a hearing, trial or other proceeding shall advise the Court at the time of introduction that the information sought to be introduced is protected. In light of the burden that the introduction of designated material imposes upon the Court, the parties are instructed to use their best efforts to limit the introduction of such material and the continued designation of such material as confidential in the event its introduction is necessary. If the party who designated the information as protected requests the protection be continued, the Court will review the information, *in camera*, to determine if the information is entitled to continued protection. Unless expressly ordered to be "SEALED" by the Court, any materials entitled to protection from disclosure under this Order shall maintain their Provisionally Sealed status and, be viewable only by Court personnel and Appointed Counsel for the parties, and remain subject to the restrictions on Confidential and Highly Confidential documents under this order, as applicable.

E. In the event any case is remanded, Protected Material shall be filed under seal in the transferor court according to the Electronic Case Filing procedures and other applicable rules of the transferor district and shall remain

restricted in the Clerk's office of the transferor court so long as they retain their status as Stamped Confidential Documents.

X. PROPER USE OF PROTECTED MATERIAL

Persons obtaining access to Protected Material pursuant to this Protective Order shall use the information in connection with this litigation only — including appeals and retrials — and shall not use such information for any other purpose, including business, governmental, commercial, or administrative or judicial proceedings, unless otherwise required by applicable law.

XI. NON-TERMINATION

The provisions of this Protective Order shall not terminate at the conclusion of this MDL proceeding or any or all of the individual actions coordinated or consolidated therein.

Upon written request, within 90 days after final disposition of this or any related litigation, Protected Material and all copies of same (other than exhibits of record) and information integrated into work product shall be returned to the Producing Party or destroyed. Final disposition, for purposes of this Order, is the later of: (1) dismissal of all claims and defenses in this action, with prejudice; and (2) final judgment herein after the completion and exhaustion of all appeals,

rehearing, remands, trials, or reviews of this action, including the time limits for filing any motions or applications for extension of time pursuant to applicable law.

Any return shipping done at the request of the Producing Party shall be done at the expense of the Producing Party. Notwithstanding the foregoing, counsel for all parties may keep one copy of any transcripts, pleadings and exhibits and shall maintain them in confidence. Upon written request, all counsel of record shall make certification of compliance herewith and shall deliver the same to counsel for the Producing Party not more than 100 days after final termination of this and all related litigation.

XII. NON-WAIVER OF PRIVILEGES

A. This Protective Order is entered pursuant to and invokes the protections of Federal Rule of Evidence 502(d). Accordingly, the provisions in Rule 502(b) will not apply to the disclosure of documents or information ("Discovery Material") in this action, other than an intentional disclosure. In order to allow for expeditious production of documents, a Producing Party may, at its sole option, produce such materials without detailed, or any, review to determine whether the production includes Privileged Material.

B. In accordance with Federal Rule of Evidence 502(d) and other applicable Rules, any such production or disclosure of Privileged Material other

than the knowing and intentional disclosure of a document or information, shall not be deemed to waive—in this litigation or in any other federal or state proceeding — any applicable privilege or immunity (including, without limitation, the attorney-client privilege, the work product immunity and the joint defense or common interest privilege) that would otherwise attach to the disclosed materials or their subject matter. The Parties shall not argue, in this forum or any other, that any privilege or protection was waived as a result of inadvertent disclosure in this action, regardless of the procedures used to identify Privileged Material prior to production.

C. If a Party identifies discovery material that appears on its face to be Privileged Material belonging to another Party or non-party, the identifying Party is under a good-faith obligation to notify that other Party or non-party. Such notification shall not waive the identifying Party's ability to subsequently contest any assertion of privilege or protection with respect to the identified discovery material. If the Party or non-party to which the disclosed Privileged Material belongs wishes to assert a claim of privilege or protection, that Party or non-party shall notify the receiving Party of its assertion of privilege within 7 calendar days of receiving the identifying party's notification of potentially Privileged Material. Nothing in this Stipulation and Order limits or otherwise modifies an attorney's

ethical responsibilities to refrain from examining or disclosing materials that the attorney knows or reasonably should know to be Privileged Material and to inform the disclosing Party that such Privileged Material has been produced.

D. This Stipulation and Order does not preclude a Party from intentionally waiving any claims of privilege or protection.

E. The provisions of Rule 502(a) of the Federal Rules of Evidence apply when a Party uses Privileged Material or Protected information to support a claim or defense, when a Party uses Privileged Material or Protected Information during a deposition without the assertion of a contemporaneous objection, when a Party intentionally discloses Privileged Material or Protected Information to a third party, including the Court (e.g., in connection with or support of a filing), or when a Party makes selective disclosures of documents for any other purpose. This paragraph does not preclude a Party from arguing that waiver was made under any applicable rule of law.

F. The Parties may stipulate without the need for Court approval to narrow or extend the time periods specified in this Stipulation and Order.

XIII. CLAWBACK OF DISCLOSURE

A. A Producing Party that determines that it made a disclosure of Confidential or Highly Confidential Information or Privileged Material in this

litigation shall promptly notify the Receiving Party following discovery of the production, and the Receiving Party (the "Returning Party") shall:

1. in the case of Privileged Material, (i) immediately cease the review and use of the disclosed document or information, except to the extent necessary to determine and/or contest the privilege or protection; (ii) if the Receiving Party does not challenge the assertion, return, sequester, or destroy the disclosed document or information forthwith, as well as any and all copies thereof; and (iii) if the Receiving Party does not challenge the assertion, destroy or sequester any references to the erroneously or inadvertently disclosed document or its contents, to the extent such references exist in other materials prepared by the Returning Party; or,

2. in the case of a Confidential or Highly Confidential document, shall mark it and all copies "CONFIDENTIAL — SUBJECT TO PROTECTIVE ORDER" or "HIGHLY CONFIDENTIAL — SUBJECT TO PROTECTIVE ORDER" at the expense of the Producing Party and treat the document as Protected Material under the terms of this Order. A party may sequester a Document if challenging a clawback request.[1]

Upon request of the disclosing Party, the Returning Party must provide to the disclosing Party a certification of counsel that all of the disclosed discovery has been returned, sequestered, or destroyed subject to the terms of this paragraph. The Receiving Party is not required to return, sequester, or destroy any discovery item

[1] Copies of disclosed Confidential Information, Highly Confidential Information or Privileged Material that have been stored on electronic media that are not reasonably accessible, such as disaster recovery backup media, are adequately sequestered as long as they are not restored. If such data is restored, the Returning Party must take steps to re-sequester the restored disclosed Confidential Information, Highly Confidential Information, or Privileged Material.

claimed to be Privileged Material if the Receiving Party intends to move the Court for a ruling that the document was never privileged or protected, unless and until the Court determines the document is privileged or protected.

If any produced Privileged Material, Confidential Information, or Highly Confidential Information has been provided to a non-party by a non-Producing Party, the non-Producing Party will use all reasonable efforts to secure the return of the Privileged Material (and the destruction of any references thereto) and/or proper designation of the Confidential Information or Highly Confidential Information, including reminding the non-party of its obligation to adhere to the terms of this Protective Order that non-party agreed to by executing the Acknowledgement attached as Exhibit A.

B. Notice of disclosure shall apply to all copies of the document disclosed.

C. If a Receiving Party disputes the Producing Party's privilege claim, the Receiving Party shall notify the Producing Party of the dispute and the basis therefore in writing within 10 business days of receipt of the notification of produced Privileged Information. However, to the extent that a Producing Party seeks to claw back more than 100 documents within a 7-day period, the Receiving Party shall be provided an additional 10 business day to review such documents

and dispute the privilege claims asserted over them. The Producing Party and Receiving Party thereafter shall meet and confer in good faith regarding the disputed claim within 10 business days. In the event that the Producing Party and Receiving Party do not resolve their dispute, the Party claiming privilege must bring a motion for a determination of whether a privilege applies within 10 days of the determination that no resolution will be achieved. If such a motion is made, the moving party shall submit to the Court for *in camera* review a copy of the produced Privileged Information in connection with its motion papers.

D. A Party is not precluded by this Stipulation and Order from arguing that a privilege or protection has been waived for reasons other than the production of a document or information subsequently clawed back in accordance with the terms of this Stipulation and Order.

E. Notwithstanding the foregoing, the Parties agree that any document used by any Party in a deposition, expert report, or court filing in this action (with the exception of a motion pursuant to Section XIII.C. of this Stipulated Protective Order), that a Producing Party does not claw back within 7 calendar days of its use, ("Used Document") shall not be eligible for clawback of that document under Sections XIII. A-C of this Stipulated Protective Order. Such ineligibilty for clawback of that document under Sections XIII. A-C of this Stipulated Protective Order shall not result

in a subject matter waiver in any other state or federal proceeding. The Producing Party reserves its rights to utilize FRE 502(b) and the Receiving Party reserves its rights under FRE 502(b), including but not limited to establishing whether and to what extent a court order recognizing waiver of privilege under FRE 502(b) with respect to a document effects a subject matter waiver.

F. Nothing in this Stipulation and Order is intended to preclude either party from seeking fees or expenses associated with the unreasonable or excessive Clawback of documents.

XIV. MODIFICATION PERMITTED

Any party for good cause shown may apply to the Court for modification of this Protective Order. This Protective Order shall remain in full force and effect and each person subject to this Order shall continue to be subject to the jurisdiction of this Court, for the purposes of this Order, in perpetuity, and the Court shall not be divested of jurisdiction of any person or of the subject matter of this Order by the occurrence of conclusion of this case, or by the filing of a notice of appeal, or other pleading which would have the effect of divesting this Court of jurisdiction of this matter generally.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

DATED: April 16, 2018

/s/ *Kenneth S. Canfield* W/E/P
Kenneth S. Canfield

DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E.
Suite 1600
Atlanta, Georgia 30309
Tel. 404.881.8900
kcanfield@dsckd.com

Amy E. Keller
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dlcfirm.com

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel. 816.714.7100
siegel@stuevesiegel.com

Consumer Plaintiffs' Co-Lead Counsel

Roy E. Barnes
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Tel. 770.227.6375
roy@barneslawgroup.com

David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350
Tel. 404.205.8400

david@ewlawllc.com

Consumer Plaintiffs' Co-Liaison Counsel

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500
Washington, DC 20005
Tel. 202.408.4600
afriedman@cohenmilstein.com

Eric H. Gibbs
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612
Tel. 510.350.9700
ehg@classlawgroup.com

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, DC 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Ariana J. Tadler
MILBERG TADLER PHILLIPS GROSSMAN LLP
One Penn Plaza
19th Floor
New York, New York 10119
Tel. 212.594.5300
atadler@milberg.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. 813.223.5505
jyanchunis@forthepeople.com

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224
Tel. 410.539.6500
hassan.murphy@murphyfalcon.com

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
Tel. 770.578.1314
jasondoss@dossfirm.com

Consumer Plaintiffs' Steering Committee

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, GA 30303
Tel. 404.584.9777
rodney@gspclaw.com

Consumer Plaintiffs' State Court Coordinating Counsel

/s/ *Joseph P. Guglielmo* W/E/P
Joseph P. Guglielmo

SCOTT+SCOTT ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Tel. 212.223.6444
jguglielmo@scott-scott.com

Gary F. Lynch
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Tel. 412.322.9243
glynch@carsonlynch.com

Financial Institution Plaintiffs' Co-Lead Counsel

Craig A. Gillen
GILLEN WITHERS & LAKE, LLC
3490 Piedmont Road, N.E.
One Securities Centre, Suite 1050
Atlanta, GA 30305
Tel. 404.842.9700
cgillen@gwllawfirm.com

MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Tel. 404.320.9979
mgibson@thefinleyfirm.com

Ranse Partin
CONLEY GRIGGS PARTIN LLP
4200 Northside Parkway
Building One, Suite 300

Atlanta, Georgia 30327
Tel. 404.572.4600
ranse@onleygriggs.com

Financial Institution Plaintiffs' Co-Liaison Counsel

Arthur M. Murray
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Tel. 504.525.8100
amurray@murray-lawfirm.com

Stacey P. Slaughter
ROBINS KAPLAN LLP
800 LaSalle Avenue Suite 2800
Minneapolis, MN 612-349-8500
Tel. 612.349.8500
sslaughter@robinskaplan.com

Charles H. Van Horn
BERMAN FINK VANHORN P.C.
3475 Piedmont Road, Suite 1100
Atlanta, GA 30305
Tel. 404.261.7711
cvanhorn@bfvlaw.com

Allen Carney
CARNEY BATES & PULLIAM, PLLC
519 W. 7th Street
Little Rock, AR 72201
Tel. 501.312.8500
acarney@cbplaw.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North

Suite 300
Minneapolis, MN 55401
Tel. 612.339.7300
bbleichner@chestnutcambronne.com

Karen Hanson Riebel
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Tel. 501.812.5575
khriebel@locklaw.com

Karen S. Halbert
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223
Tel. 501.821.5575
karenhalbert@robertslawfirm.us

Brian C. Gudmundson
ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Tel. 612.341.0400
brian.gudmunson@zimmreed.com

Financial Institution Plaintiffs' Steering Committee

-and-

/s/ S. Stewart Haskins II
KING & SPALDING LLP

David L. Balser
Georgia Bar No. 035835
Phyllis B. Sumner
Georgia Bar No. 692165
S. Stewart Haskins II
Georgia Bar No. 336104
Elizabeth D. Adler
Georgia Bar No. 558185
John C. Toro
Georgia Bar No. 175145
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
psumner@kslaw.com
shaskins@kslaw.com
eadler@kslaw.com
jtoro@kslaw.com

IT IS SO ORDERED.

Date: April 17, 2018

/s/Thomas W. Thrash
Thomas W. Thrash
United States District Judge

ATTACHMENT A

ACKNOWLEDGMENT OF CONFIDENTIALITY DESIGNATIONS AND AGREEMENT TO BE BOUND BY TERMS OF COURT ORDER

_____ declares that:

I reside at _____ in the City of _____, County of _____, State of _____. My telephone number is _____.

I am currently employed by _____, located at _____, and my current job title is _____.

I have read and understand the terms of the Protective Order dated _____, 2018, filed in *In re: Equifax, Inc. Data Security Breach Litigation*, Case No. 1:17-md-2800-TWT, currently pending in the United States District Court for the Northern District of Georgia. I agree to comply with and be bound by the provisions of the Protective Order. I understand that any violation of the Protective Order may subject me to sanctions by the Court.

I shall not divulge any documents, or copies of documents, designated "Confidential" or "Highly Confidential" obtained pursuant to such Protective Order, or the contents of such documents, to any person other than those specifically authorized by the Protective Order. I shall not copy or use such

documents except for the purposes of this action and pursuant to the terms of the Protective Order.

As soon as practical, but no later than 30 days after final termination of this action, I shall return to the attorney from whom I have received them any documents in my possession designated "Confidential" or "Highly Confidential," and all copies, excerpts, summaries, notes, digests, abstracts, and indices that contain Confidential or Highly Confidential Information.

I submit myself to the jurisdiction of the United States District Court for the Northern District of Georgia for the purpose of enforcing or otherwise providing relief relating to the Protective Order.

This _____ day of _____, 2018.

_____
Signature

_____
Printed Name